PERSON TO PERSON™

PERSONAL ENCRYPTION TOOL

PTP LITE USER MANUAL

© 2009 PTP Security. All Rights Reserved.

Person To Person

© 2009 PTP Security. All Rights Reserved.

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. Under no circumstances shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Revised 5th February 2010

Table of Contents

Part 1 Introduction

1 Welcome 3
2 Installation 3
3 Theory of Operation 3
4 Compatibility 4
5 Support 4

Part 2 Starting To Use PTP LITE

1 Using PTP LITE with the FREE License 5
2 Using PTP LITE with a FULL License 5
3 Working Folders 5
4 Embedded Help 5

Part 3 Using PTP LITE

1 General Usage 6
2 Change Password 6
3 Delete Contact 7
4 Create MyPublicKey 7
5 Details Button 7
6 Upgrade To Full License 7
7 Display Buttons 7
8 Cloning from PTP Standard/Plus/Pro 8
9 Identity Code 8

Part 4 About Encryption

1 Cyphermax 9
2 Identity Verification 9
3 Changing Your Password 10
4 Forgotten Password 10

© 2009 PTP Security. All Rights Reserved - Revised 2010-02-05

1 Introduction

1.1 Welcome

Person To Person allows you to encrypt and decrypt disc files and files which are to be used as email attachments, facilitating secure communications between you and your correspondents.

Person To Person (PTP) uses CypherMax™ technology to encrypt securely your data without the use of digital certificates. No third party or third party components (like certificates) are required to use PTP between yourself and other PTP users.

PTP does not require the transmission of any secret information by any means between participating parties.

PTP does not require the storage of any secret data on the PC or any associated storage medium.

Person To Person is supported on Windows 2000 and later.

1.2 Installation

The software consists of only one file, PTP.exe. This file is digitally signed by the manufacturer and self-certifies each time it runs.

When you download the file you can choose to save it onto a blank memory stick. This is the extent of the installation process. You can now run PTP on any PC without further installation and without leaving a trace on the PC.

Alternatively you can create a folder, e.g. c:\PTPLite, and save it to this.

In either case nothing in the Registry is touched.

1.3 Theory of Operation

PTP LITE is a simple Windows Dialog Box application. It requires nothing to operate that is not available as standard in every Windows-based PC. You can use any file browsing utility to place files for processing in the folder 'InBox.ptp' and retrieve the result from 'OutBox.ptp'.

When you sign a file with PTP, or create a MyPublicKey file, and send it to a contact, after it is processed by the contact it automatically creates an entry in the contact's Secure Contact List. This enables the contact to encrypt files for you - no-one but you will be able to decrypt files intended for you, not even the contact.

You can sign a file and send it to as many contacts as you like. When a contact processes your file it acts as certification that you are the source of the file. Any signed or encrypted file successfully retrieved is guaranteed to have been transmitted without change and without virus infection.

A simple one-off manual procedure allows you to eliminate the possibility of impersonation.

© 2009 PTP Security. All Rights Reserved - Revised 2010-02-05

An option is available to produce output entirely as a text document in case some contacts possess firewalls which are suspicious of binary data.

PTP LITE will only process one file at a time. If a number of files are to be encrypted or signed, they can be zipped into a single file before processing.

The FREE License version allows 25 operations for the purposes of evaluation.

1.4 Compatibility

PTP LITE is compatible with PTP Email Security with respect to single-file operation.

If it is required to process the multiple-file container of type .PTPZ produced by PTP Email Security you can use WinZip to extract the files which can then be processed separately by PTP LITE.

1.5 Support

Any issues relating to the performance of PTP LITE should be addresses to **info@ptpencryption.com**.

© 2009 PTP Security. All Rights Reserved - Revised 2010-02-05

2 Starting To Use PTP LITE

2.1 Using PTP LITE with the FREE License

Browse to the file PTP.exe on the memory stick or in the PC folder you chose to store it and run.

On first running PTP, click GO. In the Reg Data box type your USER ID (case-sensitive). Contacts will know and refer to you by this name. Now click SUBMIT.

Enter your chosen PASSWORD in the top box and click ENTER. Re-enter your PASSWORD in the top box and click ENTER. Your password should be at least 6 characters long. You will be able to achieve very high levels of security if you choose a password or pass phrase of greater length - up to 32 characters.

2.2 Using PTP LITE with a FULL License

Browse to the file PTP.exe on the memory stick or in the PC folder you chose to store it and run.

In the Reg Data box type the REGISTRATION CODE which you obtained at purchase and click SUBMIT.

In the Reg Data box type your USER ID (case-sensitive) which you supplied at purchase. Contacts will know and refer to you by this name. Click SUBMIT.

In the Reg Data box type your SETUP CODE which you obtained at purchase and click SUBMIT.

Enter your PASSWORD in the top box and click ENTER. Re-enter your PASSWORD in the top box and click ENTER. Your password should be at least 6 characters long.

2.3 Working Folders

When you run PTP LITE for the first time it creates sub-folders within the folder containing PTP.exe.

InBox.ptp
OutBox.ptp
Data.ptp

InBox.ptp is the folder in which you place the file you wish to sign or encrypt. OutBox.ptp is the folder from which you retrieve the processed file.

Data.ptp is used by the system. This and its sub-folders should not be modified.

2.4 Embedded Help

The information on how to use PTP LITE contained in this manual can be found from a series of Help pages embedded in the software.

Click the HELP button to view the next topic.

To return to the beginning, click CLEAR then HELP.

© 2009 PTP Security. All Rights Reserved - Revised 2010-02-05

3 Using PTP LITE

3.1 General Usage

Browse to the file PTP.exe on the memory stick or in the PC folder you chose to store it and run.

Enter your password in the box provided.

To Encrypt a file: Copy the file into InBox.ptp, then click your target contact in the Secure Contacts List. (You can only encrypt one file at a time. If you have more, zip them into one file.)

Check/Un-check the 'ASCII Output' check box. (An ASCII format file is larger but it passes more easily through firewalls.) Then click GO.

The result in OutBox.ptp is a file of the same name but of type .ptp.

To Sign a file, copy it into InBox.ptp. Target contact is not relevant. When a file is signed it is encrypted with a medium-strength cypher. It can be sent to anyone and anyone with PTP can decrypt it. You can password-protect it by entering a pass phrase before signing in the top right hand box . (This is different from your PTP password.)You will need to tell this to your intended contact or contacts.

To Decrypt an encrypted file or authenticate a signed file, copy it into InBox.ptp. Select Decrypt and Click GO. If it was a signed file protected by a pass phrase enter the pass phrase before decrypting in the top right box.

New encryptions or signings always overwrite the contents of OutBox.ptp. InBox.ptp is always cleared afterwards so make sure you retain a copy of your original file. InBox.ptp is always cleared after an error (such as trying to decrypt a file not for you). This can be a nuisance but is necessary to maintain security.

If you want to encrypt the same file for a different contact, please copy the file again to InBox.ptp and repeat the procedure. To encrypt a file to store for yourself, choose Myself as the contact.

3.2 Change Password

Your Password should be as long and strange as you can manage to remember. Only change it if you suspect someone else knows it since you will need to carry out additional procedures.

Click Change Password button and click GO. Enter your new Password in the top right box and click the ENTER button. Re-enter Password, click ENTER.

Then do Create MyPublicKey and send the file in OutBox.ptp to all your contacts. When they have decrypted this they will be informed of a possible password change and be prompted to contact you to verify your Identity Code. See below for more details of Identity Code.

© 2009 PTP Security. All Rights Reserved - Revised 2010-02-05

3.3 Delete Contact

You can have up to 998 entries in your list. It is updated automatically each time you receive one or more files from a new contact. To remove a contact:

Click on the contact in the Secure Contacts List.
Click on the Delete Contact button.

3.4 Create MyPublicKey

Use this to create the file MyPublicKey.ptp. Send this to your colleagues the first time you contact them. When this file has been decrypted you will be in their Secure Contacts List. Alternatively, any signed or encrypted file from you will do the same job.

3.5 Details Button

Click on a contact in the list. Click the DETAILS button.

The Contact ID is the name of the contact. The Identity Code is derived from the contact's public key by an irreversible mathematical function. See below for further information.

The Set-Up Date states when the contact initialised the software.

3.6 Upgrade To Full License

If you have been running with a FREE license and have purchased a FULL license, once you have entered your Password, enter the following into the Reg Data box and click SUBMIT:

upgrade

In the Reg Data box type the REGISTRATION CODE which you obtained at purchase and click SUBMIT.

In the Reg Data box type your USER ID (case-sensitive) which you supplied at purchase. Contacts will know and refer to you by this name. Click SUBMIT.

In the Reg Data box type your SETUP CODE which you obtained at purchase and click SUBMIT.

Enter your PASSWORD in the top box and click ENTER. Re-enter your PASSWORD in the top box and click ENTER.

3.7 Display Buttons

IN BOX:	Display InBox.ptp contents
OUT BOX:	Display OutBox.ptp contents
CLEAR:	Clear Display/Reset Help page

© 2009 PTP Security. All Rights Reserved - Revised 2010-02-05

3.8 Cloning from PTP Email Security

If you have installed PTP Email Security on your PC, you can create a PTP Lite System having the same registration, password and contacts.

Create a FREE PTP Lite system and use the Export Database function in PTP Email Security to create a .ptpdb file. Place this in the PTP Lite Inbox.ptp and decrypt. Exit and login with the PTP Email Security password.

3.9 Identity Code

Following a Decrypt Function you may be prompted to verify the Identity Code with the sender. Click the sender in the Secure Contacts List. Click the DETAILS button.

Ask for the Identity Code from the sender's 'Myself' details. Do not disclose the Identity Code you are verifying.

By trusting the sender's voice or e-mail address you are guaranteed that the sender is genuine. The Identity Code is a crucial part of the security. It is derived using a one-way function of the user's public key.

You use a trusted channel such as a voice conversation or e-mail address to verify the Identity Code. This prevents impersonation of a user's identity.

© 2009 PTP Security. All Rights Reserved - Revised 2010-02-05

4 About Encryption

4.1 Cyphermax

Cyphermax™ is a proprietary data encryption technology that combines both Public Key and Symmetric Cryptography to realise the major objectives of properly secure communications. These are the use of high strength encryption keys and the elimination of the need to transfer or store any secret data thus providing protection against message interception and loss of data or computers.

Cyphermax employs RSA public/private key pairs and a proprietary high-strength symmetric encryption algorithm for encrypting the bulk of the data

A profound development is the elimination of Digital Certificates while realising the functions they perform by other means which do not involve the user in any way. Digital Certificates require the user to disclose personal details to a third party - a certification authority - who retains these on a database. The issued certificate has a cost and an expiry date. It contains a secret part which must be retained on the user's PC. The three elements of cost, vulnerability and management overhead present a barrier to potential users few people are prepared surmount.

CypherMax is not dependent on any underlying Microsoft or any other encryption services.

4.2 Identity Verification

One of the reasons for digital certificates and certification authorities, and all the complexity these entail, is identity verification to prevent impersonation. Identity Verification in PTP employs a manual method to perform this function.

When you receive a MyPublicKey file or Signed or Encrypted file from a new contact you can use the Details button to display the contact's identity and Identity Code. It is assumed that you know enough about the contact to communicate personally. By asking them similarly to display their Identity Code (details of 'Myself') you can be sure their is no impersonation.

This is the Person to Person trust establishment system. It provides identity authentication and handles with minimum fuss password changes, re-registrations etc. It performs the same function as a digital certificate system where a third party vouches for your identity with signed certificates.

© 2009 PTP Security. All Rights Reserved - Revised 2010-02-05

4.3 Changing Your Password

WARNING

Even though you are unaware of them, you have your own Public/Private key pair. These are partially based on your database Password. Therefore, if you change your password, your keys will also change. This means that files encrypted with the old password can no longer be decrypted. It also means your public key information stored in all your contacts' databases can no longer be used to decrypt or verify files sent by you and you can no longer decrypt files sent by them.

So if you wish to change your password, you must first decrypt any files you have encrypted for yourself and re-encrypt them after changing your password.

You must also send new 'MyPublicKey' files to your contacts after changing your password.

For these reasons, **you should only change your password if you have reason to believe it has been compromised.**

4.4 Forgotten Password

There is no way round this and you will unfortunately have to start again. Run the program and enter into the password box:

forgotten password

For the **FREE License** version:

In the Reg Data box type your USER ID (case-sensitive). Now click SUBMIT.

Enter your chosen PASSWORD in the top box and click ENTER. Re-enter your PASSWORD in the top box and click ENTER.

For the **FULL License** version:

In the Reg Data box type the REGISTRATION CODE which you obtained at purchase and click SUBMIT.

In the Reg Data box type your USER ID (case-sensitive) which you supplied at purchase. Contacts will know and refer to you by this name. Click SUBMIT.

In the Reg Data box type your SETUP CODE which you obtained at purchase and click SUBMIT.

Enter your PASSWORD in the top box and click ENTER. Re-enter your PASSWORD in the top box and click ENTER.

Then:

Produce a MyPublicKey.ptp file (Create MyPublicKey function). Send this to all your contacts with a request first to remove you from their Secure Contacts Lists. After processing the file, each will be prompted to contact you to verify your new Identity Code.

© 2009 PTP Security. All Rights Reserved - Revised 2010-02-05